IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	)	Civil Action No. 1:23-cv-09518-PAE **ORAL ARGUMENT REQUESTED**

THE PARTIES' JOINT STATEMENT OF UNDISPUTED FACTS[1]

I. Defendants

A. SolarWinds

1. SolarWinds Corporation ("SolarWinds" or the "Company") is a Delaware corporation with its headquarters in Austin, Texas.

2. The SEC has defined the relevant period for its claims as spanning from October 18, 2018—when SolarWinds executed its second public offering—through January 12, 2021 (the "Relevant Period").

3. During the Relevant Period, SolarWinds' stock was registered with the Securities and Exchange Commission (the "Commission") pursuant to Section 12(b) of the Securities Exchange Act of 1934 and was traded publicly on the New York Stock Exchange under the ticker "SWI."

[1] The SEC wishes to note that, in agreeing that a particular fact is undisputed for purposes of this joint statement, a party is not conceding that such fact is relevant or material for purposes of summary judgment or that any evidence upon which the fact is based is admissible. Moreover, in not a disputing a fact, a party is not affirmatively attesting to the fact, but rather is simply not disputing it for purposes of summary judgment.

4. SolarWinds is a provider of network monitoring software, offering solutions designed to provide organizations, including small businesses, large enterprises, and government organizations, with a comprehensive and unified view of their network environments.

5. SolarWinds had during the Relevant Period, and continues to have today, over 300,000 customers, including nearly all Fortune 500 companies.

6. SolarWinds had approximately 2,700–3,300 employees during the Relevant Period.

7. Founded in 1999, SolarWinds conducted its first initial public offering ("IPO") in 2009 and remained a public company until February 2016, when it was acquired by several private equity firms in a take-private transaction. SolarWinds conducted a second IPO on October 18, 2018 and remained a public company during the Relevant Period.

8. On February 7, 2025, SolarWinds announced that it entered an agreement to be privately acquired, which became effective on April 16, 2025.

B. Timothy G. Brown

9. Timothy G. Brown is a resident of Salado, Texas.

10. Mr. Brown has more than thirty years of experience in software development and cybersecurity.

11. Mr. Brown was hired by SolarWinds in July 2017.

12. Prior to that, Mr. Brown was the Chief Technology Officer at Dell, Inc., where he had responsibility for Dell's portfolio of security products and services. While at Dell, Mr. Brown was selected as a "Dell Fellow"— a peer-reviewed recognition reserved for Dell employees who have made sustained contributions to the company through their technical achievements, engineering contributions, and advancement of the industry.

13. Mr. Brown has 18 patents in the cybersecurity field for which he is the inventor.

14. Mr. Brown has been a regular speaker at industry conferences relating to cybersecurity during his career, including during the Relevant Period.

15. Mr. Brown's position when he was hired by SolarWinds in July 2017 was Vice President of Security and Architecture. His responsibilities in this position included, among other things: supervising SolarWinds "InfoSec" team, which was responsible for monitoring SolarWinds' network for security threats and responding to security incidents; and working with SolarWinds' software design teams on building security into product architecture.

16. Beyond supervising the InfoSec team and working with software design teams on building security into product architecture, Mr. Brown's role also included working to educate customers of SolarWinds' managed service provider ("MSP") business on cybersecurity best practices that they could incorporate into the services they provided to their clients. MSPs are businesses that provide outsourced information technology ("IT") services to other businesses (typically small to medium sized businesses). SolarWinds provided software and services to MSPs that the MSPs included in the package of offerings they provided to their clients in turn. As part of Mr. Brown's educational role with respect to SolarWinds MSP customers, Mr. Brown made public blog posts and other publicly available statements about cybersecurity.

17. As Vice President of Security and Architecture, Mr. Brown was not a C-suite level executive. Throughout the Relevant Period, Mr. Brown reported to the Chief Information Officer ("CIO"), Rani Johnson, who in turn reported to the Chief Technology Officer ("CTO"), Joe Kim, who in turn reported to the Chief Executive Officer.

18. During the Relevant Period, Ms. Johnson and Mr. Brown met on a quarterly basis with Mr. Kim, SolarWinds' General Counsel Jason Bliss and Chief Financial Officer ("CFO")

Bart Kalsu to discuss cybersecurity risks at SolarWinds, initiatives to address those risks, and SolarWinds' progress in addressing various cybersecurity risks.

19. After the Relevant Period, in January 2021, Mr. Brown was promoted to Chief Information Security Officer—at the time, a newly created position at SolarWinds and a role which he has since held. Mr. Brown's job responsibilities did not change as a result of the change in title.

C. Other Relevant SolarWinds Personnel

20. Rani Johnson was SolarWinds' CIO between February 2017 and October 2020. In that role, she supervised all of SolarWinds' internal IT operations. She directed a staff of approximately 300 persons, which included the InfoSec team led by Mr. Brown.

21. Beyond Mr. Brown, another of Ms. Johnson's direct reports was Brad Cline, who served as a Senior Manager of IT and then a Director of IT from October 2016 to November 2019, and (after a short stint at another company) as a Senior Director of IT from October 2020 through the end of the Relevant Period. Mr. Cline was in charge of several teams, including: the Networking team, which managed all of SolarWinds' internal network and connections to cloud-based services the Company used (such as Amazon Web Services); the Server team, which managed the servers used in the Company's operations; and the End-user Services team, which was responsible for providing IT assistance to SolarWinds' employees, including provisioning and de-provisioning them with access as part of the onboarding and offboarding process.

22. During the Relevant Period, Ms. Johnson reported directly to Mr. Kim, who was the CTO of SolarWinds between February 2016 and November 2020. In that role, in addition to overseeing the internal IT operations supervised by Ms. Johnson, Mr. Kim oversaw the software architecture and engineering teams that designed and developed the Company's software products.

23. Eric Quitugua has worked at SolarWinds in an information security capacity since June 2015. During the Relevant Period, he managed the InfoSec team under Mr. Brown, to whom he directly reported.

24. Steven Colquitt was a Director of Software Engineering at SolarWinds during the Relevant Period, within Mr. Kim's organization.

II. The Security Statement

25. SolarWinds posted a document entitled "SolarWinds Security Statement" on its publicly available website on November 16, 2017 (the "Security Statement"), almost one year before SolarWinds' IPO.

26. A copy of the Security Statement, as it appeared throughout the Relevant Period, is attached as Exhibit A.

27. At the time the Security Statement was posted in 2017, it was becoming increasingly common for companies to conduct some level of cybersecurity diligence on their software vendors as part of their procurement processes.

28. Prior to the posting of the Security Statement, SolarWinds' general practice was to respond to customers' questions about SolarWinds' cybersecurity practices individually over email.

29. Over time, SolarWinds had developed a database of security-related questions asked by customers, along with answers that had been vetted by relevant subject-matter experts in the Company and approved by the Legal department.

30. In mid-2017, SolarWinds decided to publish answers to commonly asked questions to a page on its website—the Security Statement—so that customers could find these answers online on their own.

31. Mr. Brown was in favor of publishing the Security Statement on SolarWinds' website for this purpose, as were his supervisors. The Security Statement was drafted by Eric Quitugua, who worked under Mr. Brown.

32. Mr. Quitugua drafted the Security Statement by consolidating content from the Company's preexisting database of answers to customer security-related questions.

33. To the extent Mr. Quitugua needed any additional information about a topic in the Security Statement, he consulted with the relevant subject-matter expert(s) at the Company.

34. Mr. Quitugua provided his draft of the Security Statement to Mr. Brown, who reviewed it along with Ms. Johnson, Mr. Kim, as well as the Legal department, before it was published.

35. Mr. Brown, Ms. Johnson and Mr. Kim were all makers of the Security Statement for purposes of *Janus Capital Group, Inc. v. First Derivative Traders*, 564 U.S. 135 (2011).

36. Mr. Brown does not recall making any substantive edits to the Security Statement, and there is no record of him doing so.

37. The version of the Security Statement that was ultimately published on SolarWinds' website was close to the language drafted by Mr. Quitugua.

38. Companies often apply different levels of cybersecurity diligence to different vendors—depending on, for example, how important each vendor is to the company's business and what level of access it has to the company's data.

39. The Security Statement provided the sort of information about SolarWinds' cybersecurity program that was generally sought by companies seeking to do a relatively low level of diligence on SolarWinds' security practices.

40. Companies that required more extensive diligence continued to send SolarWinds detailed questionnaires after publication of the Security Statement, which SolarWinds continued to answer. SolarWinds had a more detailed version of the Security Statement, prepared around the same time as the online Security Statement, that it used to answer these more detailed inquiries. In order to protect this more sensitive information, SolarWinds would typically only provide such additional detail to customers after the customer signed a non-disclosure agreement.

III. The NIST Cybersecurity Framework

41. Under the heading titled, "Organizational Security," the Security Statement stated, "SolarWinds follows the NIST Cybersecurity Framework with layered security controls to help identify, prevent, detect, and respond to security incidents."

42. The NIST Cybersecurity Framework ("NIST CSF") is a resource published by the National Institute for Standards and Technology ("NIST"), which is housed within the U.S. Department of Commerce.

43. The NIST CSF was first published in 2014.

44. The version of NIST CSF that was in place during the Relevant Period was version 1.1. *See Framework for Improving Critical Infrastructure Cybersecurity Ver. 1.1* ("NIST CSF 1.1"), NIST (Apr. 16, 2018) at 3, https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.

45. The NIST CSF is a voluntary framework intended to help organizations identify, assess, and manage their cyber risks. *See* NIST CSF 1.1 at v.

46. The NIST CSF "can be used by organizations in any sector of the economy or society. It is intended to be useful to companies, government agencies, and not-for-profit organizations regardless of their focus or size." *See* NIST CSF 1.1 at 3.

47. The NIST CSF is not a cybersecurity "standard"—that is, it does not prescribe particular controls that an organization must adopt in order to "comply."

48. Rather, the NIST CSF "offers a flexible way to address cybersecurity," through a self-assessment process designed to "help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources." *See* NIST CSF 1.1 at v-vi.

49. As it explains, the NIST CSF establishes "a common taxonomy and mechanism for organizations to:

1) Describe their current cybersecurity posture;

2) Describe their target state for cybersecurity;

3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;

4) Assess progress toward the target state;

5) Communicate among internal and external stakeholders about cybersecurity risk."

See NIST CSF 1.1 at 2.

50. The NIST CSF divides cybersecurity activities into five "Functions": "Identify, Protect, Detect, Respond, Recover." *See* NIST CSF 1.1 at 3.

51. These "five high-level Functions . . . provide a concise way for senior executives and others to distill the fundamental concepts of cybersecurity risk so that they can assess how identified risks are managed, and how their organization stacks up at a high level against existing cybersecurity standards, guidelines, and practices. The Framework can also help an organization answer fundamental questions, including 'How are we doing?' Then they can move in a more informed way to strengthen their cybersecurity practices where and when deemed necessary." *See* NIST CSF 1.1 at 13-14.

52. Within each Function, the Framework lists categories and subcategories of cybersecurity objectives. *See* NIST CSF 1.1 at 23-24.

53. An organization using the Framework can rate itself within these categories by selecting a numerical score—or "Tier"—for its controls in each category. *See* NIST CSF 1.1 at 8-11.

54. "Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices." *See* NIST CSF 1.1 at 8.

55. The Framework does not require an organization to meet any particular Tier—*i.e.*, it does not require any minimum scores. *See* NIST CSF 1.1 at 8-11.

56. Rather, "Tiers are meant to support organizational decision making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and could receive additional resources." *See* NIST CSF 1.1 at 8.

57. Under the Framework, organizations are free to select which NIST CSF categories and subcategories to evaluate, and may even create their own categories to fit their particular business and cybersecurity needs. *See* NIST CSF 1.1 at 22.

58. There is no particular level of formality or comprehensiveness that an organization must follow in applying the Framework.

59. "The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure." *See* NIST CSF 1.1 at vi.

60. "To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization." *See* NIST CSF 1.1 at vi.

61. "For example, one organization may choose to use the Framework Implementation Tiers to articulate envisioned risk management practices. Another organization may use the Framework's five Functions to analyze its entire risk management portfolio; that analysis may or

may not rely on more detailed companion guidance, such as controls catalogs." *See* NIST CSF 1.1 at vi.

62. Following the NIST CSF does not imply that an organization meets any particular controls.

63. Organizations using the NIST CSF are free to consult other, more detailed technical references as "informative references" in selecting specific outcomes they may wish to achieve under particular NIST CSF subcategories. NIST Special Publication 800-53 is an example of one such "informative reference." NIST guidance explains that "[u]se of Informative References is non-compulsory for Framework implementation" and that even where they are used "they should not be viewed as a checklist that must be completed to implement the subcategory outcome." "Organizations have the flexibility to mix and match Informative References as best suits their needs. They may use all, some, none, or even choose to map additional practices not included in the Informative References catalog." *See* NIST.gov, *Informative References: What are they, and how are they used?*, Jan. 11, 2019, https://web.archive.org/web/20190111130000/https://www.nist.gov/cyberframework/online-learning/informative-references.

64. During the Relevant Period, SolarWinds used the NIST CSF as guidance in evaluating its cybersecurity program.

65. In August 2017, Mr. Quitugua prepared what he described in an email as "an assessment of the state of our security program" that was based on "security controls mapped to the NIST Cybersecurity framework." The spreadsheet attached to the email reflects a set of security categories and subcategories organized under the five NIST Functions, as to which Mr. Quitugua had assigned numerical scores.

66. In the fall of 2018, Mr. Quitugua prepared another self-assessment, in the form of a spreadsheet titled "SolarWinds Security Program Assessment," which contained a set of security categories and subcategories under the five NIST Functions, as to which Mr. Quitugua assigned numerical scores.

67. In 2019, Ms. Johnson and Mr. Brown began a practice of preparing "NIST Scorecards" to present in quarterly briefings to management.

68. These scorecards reflected evaluations by Mr. Brown and Ms. Johnson of SolarWinds' "NIST Maturity Level" in categories of cybersecurity activities organized under the five NIST Functions.

69. The scorecards were included in larger slide decks titled "Quarterly Risk Reviews" that were drafted with input from Mr. Brown and Ms. Johnson and were presented on a quarterly basis in person by Mr. Brown and Ms. Johnson to executive management, including the Company's General Counsel, Jason Bliss, Chief Technology Officer, Joseph Kim, and Chief Financial Officer, Bart Kalsu. The scorecards were created to provide a high-level update on the status of the Company's cybersecurity program and the planned or ongoing improvement projects it was pursuing.

70. This practice continued through the end of the Relevant Period.

IV. ROLE-BASED ACCESS CONTROLS

71. Under a heading titled, "Access Controls," the Security Statement stated the following:

> **Role Based Access**
>
> Role based access controls are implemented for access to information systems. Processes and procedures are in place to address employees who are voluntarily or involuntarily terminated. Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary

> basis. Access control lists define the behavior of any user within our information systems, and security policies limit them to authorized behaviors.
>
> **Authentication and Authorization**
>
> . . .
>
> SolarWinds employees are granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet. Employees are granted access to certain additional resources based on their specific job function. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as defined by our security guidelines. Approvals are managed by workflow tools that maintain audit records of changes.

72. Role-based access controls are measures designed to provision users with access to systems based on what they need to perform their roles.

73. The principle of least privilege access is a related concept that refers to the principle of provisioning users with the minimum access needed to perform their duties.

74. During the Relevant Period, SolarWinds had a process in place designed to provision users with access based on what they needed for their role, referred to internally by the company as the "SARF process."

75. As part of the SARF process, the Company's routine practice[2] for provisioning a new employee with access rights was as follows: The employee's manager would fill out a form—known as a "System Access Request Form" or "SARF"—on which the manager would identify the employee's role at the company. Based on the employee's identified role, SolarWinds' IT department would then provision the employee with a certain set of access rights designated for

[2] Where this document references a "routine practice," the actions that are described as part of that practice (e.g., the conduct described in this paragraph after "as follows") are actions that the Company would have regularly or typically performed in carrying out the practice. It does not mean that the actions were necessarily performed perfectly or without fail.

that role—on top of a limited set of access rights that all employees would receive for basic company resources, such as email and the corporate intranet.

76. The form of the SARF changed during the Relevant Period.

77. A sample of the SARF as it existed from 2018 to mid-2019 (the "SARF 1.0 Form") is attached as Exhibit B.

78. As indicated on the SARF 1.0 Form, there were dozens of different types of roles that were defined for purposes of provisioning employees with access rights.

79. For example, the SARF 1.0 Form specifies the following access rights for someone in the "Marketing – Demand Generation" role:

> **Marketing – Demand Generation**
> Netsuite – SW Marketing Admin (upon request)
> Salesforce.com - Marketing User
> MicroSoft Vizio
> Silverpop / Marketo
> LiveBall

80. This indicates that an employee in this role should receive access to the applications listed—Netsuite, Salesforce.com, MicroSoft Vizio, Silverpop / Marketo, and LiveBall. It also indicates that, for Salesforce.com, the level of access granted should be that of a "Marketing User," and for Netsuite, the level of access would be that of a "SW Marketing Admin," if requested.

81. For other roles, the SARF 1.0 Form provided different lists of standard systems and access levels, such as in the following examples:

> **IT – Security Team**
> Netsuite – SW Helpdesk
> Web Helpdesk – Tech access
> Additional accesses to be requested based on role
>
> **Senior Finance (Controllers and Treasury)**
> Netsuite – Global Accountant & access corresponding to job duties
> On-line banking – as approved
> Solium Transcentive – Read Access (as approved)
>
> **R&D – QA & Testers**
> Netsuite – SolarWinds Support Person
> Fogbugz / Jira

Active Directory – SWDEV account
Tableau – QA Managers & above
Perforce – upon request
Go to Meeting account – Managers & above
Testlink account
VM & vSphere

82. SolarWinds also maintained written policy documentation about the SARF process that included a "Systems Group Matrix" setting forth a matrix of roles along with the "standard system accesses" designated for each role.

83. A sample of the SARF as it existed after mid-2019, which was an online form ("the SARF 2.0 Form"), is attached as Exhibit C.

84. With the SARF 2.0 Form, the access rights associated with a particular role could be found through entering the employee's region, business, unit, function, and team in the online form, which would bring up the "role-defined accesses" designated to be "provisioned for the new hire by default."

85. For example, for an employee in the "IT Help Desk" function, in the "DOIT / Architecture / UX & Engineering" team, in the "G&A" business unit, the online form would list the following access rights:

Application | Portal	**Permission Level**	**Provisioning Group**
Active Directory	Standard User	EUS
SolarHR	Standard User	HROps
Saba	Standard User	HROps
Web HelpDesk	Standard User	Infrastructure Engineering
Confluence	Standard User	EUS
Coupa	Standard User	Business Applications
Office 365	Standard User	EUS

CIMS	Standard User	HROps
Bswift	Standard User	HR Comp
Egencia	Standard User	Corporate Travel
JIRA	Standard User	Engineering Ops
Web HelpDesk	Help Desk: (L1) Access	Infrastructure Engineering
Exchange	Help Desk: (L1) Access	Infrastructure Engineering
Office 365	Help Desk: (L1) Access	Infrastructure Engineering
Access Rights Management	Standard User	

86. In the above chart, the "Application / Portal" column indicates the resources to which the user should receive access: as a routine practice, the "Permission Level" denotes the level of privilege the user should receive as to that resource; and the "Provisioning Group" denotes the name for the group of users to which the user should be added in order to assign the user the listed access rights.

87. In addition to the standard access assignments that were defined for each role, the SARF (both versions of it) allowed the employee's manager to specify any non-standard systems that the employee also needed access to, which required special approval by a data or system owner or manager.

88. Absent such special approval, the employee was only entitled to receive access to the standard systems designated for their role.

89. SolarWinds' routine practice in implementing a SARF for a new employee was as follows: When the SARF form was completed, it would be sent to IT support personnel, who in

turn would work to provision the employee with access rights based on the information in the SARF. IT support personnel would do this by generating "tickets" on SolarWinds' IT help-desk platform, which would include a copy of the SARF and would be used to track the steps taken to implement the access rights being provisioned. At a technical level, IT support staff would grant the employee access to the relevant systems by adding the employee to the access control lists governing those systems.

90. SolarWinds' routine practice was also to use the SARF process when an employee changed roles within the Company: A SARF requesting the change would be prepared and submitted to IT support staff, which would generate workflow tickets that would track implementation of the changes.

91. SolarWinds' routine practice was also to use the SARF process when an employee was terminated: IT support staff would be notified of the termination, and a ticket would be created to track the termination of their access rights.

92. The SARF process was followed as a routine practice by SolarWinds during the Relevant Period.

93. Thousands of SARFs and corresponding help-desk tickets were generated during the Relevant Period, which reflect user access rights being added, changed, or removed as part of the SARF process.

94. As part of the SARF process, SolarWinds' routine practice was to grant users administrative access rights to sensitive systems only if those rights had been determined necessary for their role.

95. Beyond the SARF process, SolarWinds also had technical processes in place to prevent employees from improperly being granted administrative access to network resources.

Specifically, SolarWinds' InfoSec team used a tool known as "Security Event Manager" or "SEM," to monitor SolarWinds' network, which was configured to detect if a user was added to a user group on the network that had administrative privileges, and, if so, to send an alert to the InfoSec team. These alerts did not automatically block the grant of administrative privileges, but instead, following such an alert, the InfoSec team's routine practice was to confirm whether the change in access rights was "authorized and intentional," by conferring with others or by finding the corresponding help-desk ticket approving the change.

96. SolarWinds had a regular practice of conducting "User Access Reviews" during the Relevant Period, for the purpose of ensuring that user access rights were appropriately configured.

97. These User Access Reviews were completed as a routine practice on a quarterly basis by SolarWinds' IT team, which would inventory user access control lists on key systems to confirm that access privileges were appropriately assigned—and to catch any potential errors that might have been made in the provisioning or de-provisioning process.

98. SolarWinds' processes for provisioning users with access were also reviewed on multiple occasions by outside auditors during the Relevant Period.

99. Specifically, as part of Sarbanes-Oxley Act ("SOX") audits conducted in 2019 and 2020, SolarWinds' outside auditor, PricewaterhouseCoopers ("PwC"), evaluated certain of SolarWinds' "IT General Controls" or "ITGCs," which are controls on a company's network that relate to the security of systems relevant to financial reporting.

100. In relevant part, PwC evaluated whether the following ITGCs with respect to user access were in place:

2.0	User Access Policy	A user access management policy is established and documented for initiating, authorizing, recording, processing, reviewing a request for access rights, and evidence retention. The user access management policy is reviewed and approved annually by the VP of IT. Evidence of review is documented and retained.

2.2	Access Provisioning	New users are provisioned access in accordance with the SolarWinds System Groups Matrix. Any additional access required, including access to super user or admin responsibilities, require approval from manager, IT and/or the system owner. Additional NetSuite access to sensitive worldwide financial results requires approval by the Financial Controller or the VP of WW Finance.
2.3	Termination	When an employee is terminated, access to Active Directory and financial systems is removed in a timely manner, as follows: - within 24 hours for administrator access - within 7 days for all other levels of access
2.5	Access Reviews	User access privileges are re-validated on a quarterly basis to confirm that users maintain appropriate access. These validation procedures are performed for all financially significant applications, systems (including Active Directory users) and databases.

101. The "SolarWinds Systems Group Matrix" listed in the "Access Provisioning" control refers to the matrix of employee roles used in the SARF process that maps each role to a specific sets of access rights needed for that role.

102. The references to "Active Directory" in the ITGCs are to a Microsoft service that is used to centrally manage user access on a Windows-based network. Active Directory was the primary tool that SolarWinds used to manage users' access rights on the Company's internal network. Because Active Directory controlled access to financial systems within the scope of the SOX audits, the PwC auditors examined the Company's processes for provisioning users with access rights through Active Directory.

103. Upon completion of the 2019 and 2020 SOX audits, PwC did not identify any material weakness or significant deficiency with respect to these controls.

104. Separately, during the Relevant Period, SolarWinds engaged several other outside accounting firms to conduct SOC-2 audits specific to several of its product lines.

105. SOC-2 audits are cybersecurity assessments that are sometimes requested by software customers seeking the security diligence for a specific product.

106. Certain of these SOC-2 reports addressed the implementation of role-based access controls for the systems that were within the scope of the assessments (which included the IT systems and infrastructure supporting the SolarWinds product being evaluated).

107. For example, a SOC-2 report prepared for SolarWinds' Database Performance Management System application, covering the period from October 1, 2019, to March 31, 2020, contained the following table:

Control Number	SolarWinds' SOC 2 Type 2 Controls	Independent Service Auditor's Test	Results
CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	A formal process is followed when provisioning new user accounts. A user access form is completed and approved by a manager before access is provisioned.	Inspected the user access forms for a selection of new employees to determine whether a formal process was followed when provisioning new user accounts and the form was completed and approved by a manager.	No exceptions noted.
CC6.3.2	Identity and Access Management (IAM) Groups are utilized within AWS to manage access to systems.	Inspected the IAM groups in the DPM AWS environment to determine whether IAM Groups were in place to manage access.	No exceptions noted.
CC6.3.3	Administrative access to the production environment is limited to appropriate personnel based on job function.	Inspected production access reviews for a selection of quarters to determine whether administrative access to the production environment was limited to appropriate personnel based on job function.	No exceptions noted.
CC6.3.4	Quarterly access reviews are performed over production systems to restrict access to authorized personnel. Inappropriate access is removed as a result of the review.	Inspected the quarterly access reviews over production systems for a selection of quarters to determine whether quarterly audits were performed and inappropriate access was removed as a result of the review, if applicable.	No exceptions noted.
CC6.3.5	Terminated employee access is revoked upon termination and documented within a termination user access form.	Inspected termination user access forms and AWS account event history for a selection of terminated employees to determine whether terminated user access forms were completed and access was revoked upon termination. Inspected production system user access lists and cross-referenced them against a selection of terminated employees to determine whether production system user accounts were revoked for terminated employees.	No exceptions noted. No exceptions noted.

108. As another example, a SOC-2 report prepared by a different outside auditor, relating to a different SolarWinds application, "Loggly," covering the period from May 1, 2020, to October 31, 2020, likewise reviewed both the design and operating effectiveness of various

controls, and made similar findings. These included opinions that: "Production servers and databases supporting the Loggly application require individual role-based accounts"; and "Access to privileged accounts in the Company's production IT systems is restricted to a limited number of SRE and Engineering personnel."

V. PASSWORDS

109. Under the "Access Controls" heading, beneath a sub-heading titled "Authentication and Authorization" the Security Statement stated as follows:

> We require that authorized users be provisioned with unique account IDs. Our password policy covers all applicable information systems, applications, and databases. Our password best practices enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords.

A. Unique User IDs

110. SolarWinds had processes in place to provision users on its network with unique account IDs, *i.e.*, usernames, during the Relevant Period.

111. A user's username would typically consist of their first and last name separated by a dot, or some other variation of the user's name, such as their first initial followed by their last name.

B. Password Policy

112. Throughout the Relevant Period, SolarWinds had in place "Enterprise Information Security Guidelines." This document "define[d] the security controls that should be in place for the environment that stores or processes personal data." This included, among other things, password requirements for "endpoints that access, store, manage, or process data," "networks that access or store data," "systems or applications that host or manage data," "in-house applications that access, manage, or store data," and "third party applications that access, manage or store data."

113. The password requirements described in the "Enterprise Information Security Guidelines" included, among other things, that passwords meet the following parameters:

3.7. Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.

3.7.1. Passwords must be at least 8 characters in length.

3.7.2. Passwords must contain characters from three of the following four categories:

3.7.3. English uppercase characters (A through Z).

3.7.4. English lowercase characters (a through z).

3.7.5. Base 10 digits (0 through 9).

3.7.6. Non-alphabetic characters (for example, !, $, #, %).

114. As part of security training that SolarWinds employees would receive as a routine practice during onboarding, employees would be informed of SolarWinds' password policy.

C. Enforcement of Complex Passwords

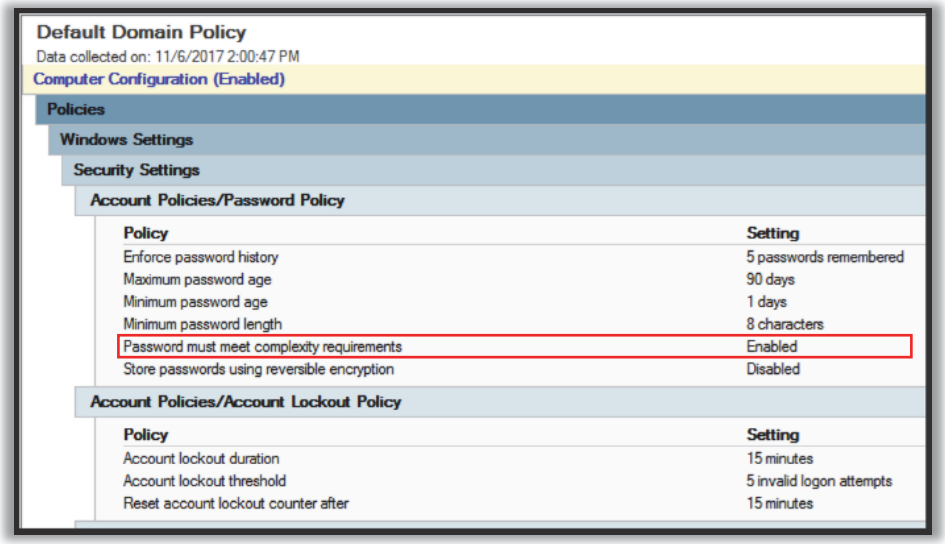
115. Enforcing password complexity automatically—so that it is not possible for a user to create a non-complex password—is a best practice.

116. However, not all IT systems have functionality that enables password complexity to be automatically enforced on user accounts on the system.

117. SolarWinds' routinely enforced password complexity automatically on systems that had such functionality.

118. In particular, SolarWinds enforced password complexity automatically on Active Directory, which was the gateway to applications on the Company's internal network.

119. A screenshot of the relevant Active Directory setting from November 6, 2017, is as follows:



Default Domain Policy
Data collected on: 11/6/2017 2:00:47 PM
Computer Configuration (Enabled)
Policies
Windows Settings
Security Settings
Account Policies/Password Policy

Policy	Setting
Enforce password history	5 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	15 minutes

120. Per Microsoft guidance from the time, enabling this setting was a "best practice" that automatically enforced certain password requirements on systems accessed through Active Directory—the same requirements set forth in SolarWinds written password policy set forth above (¶ 113). *See Password must meet complexity requirements, Microsoft* (Nov. 27, 2017), https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994562(v=ws.11).

121. Active Directory controlled access to most systems used by SolarWinds employees, so enabling the password complexity setting on Active Directory ensured that most systems used by SolarWinds employees were only accessible using a complex password.

122. As part of the SOX audits conducted by PwC during the Relevant Period, PwC evaluated whether SolarWinds "maintain[ed] password requirements for all financially significant systems and databases, including the requirements that they be changed periodically, meet minimum length requirements, retain password history, and require password complexity, as allowed by the application, system, or database."

123. As part of auditing this control, PwC interviewed SolarWinds IT personnel and reviewed sample evidence relating to implementation of password requirements, including on Active Directory as well as financially significant systems that had their own "system-specific password policy."

124. PwC did not find any material weakness or significant deficiency with respect to this control in 2019 or 2020.

125. Separately, in connection with the SOC-2 audits conducted during the Relevant Period (¶ 107), other outside accounting firms assessed password controls with respect to systems used to develop the products that were being assessed. For example, the SOC-2 audit prepared for the Database Performance Management System application mentioned above (¶ 107) validated that "SolarWinds enforces password requirements" for the systems in scope of the audit "through AWS [Amazon Web Services] Resource Groups and password requirements adhere to SolarWinds access control policy requirements."

126. There is no evidence that the use of non-complex passwords was a frequent problem at SolarWinds during the Relevant Period.

VI. NETWORK MONITORING

127. Under the "Operational Security" heading, the Security Statement stated as follows:

> **Change Management**
>
> Changes to information systems, network devices, and other system components, and physical and environment changes are monitored and controlled through a formal change control process. Changes are reviewed, approved, tested and monitored post-implementation to ensure that the expected changes are operating as intended.
>
> **Auditing and Logging**
>
> Network components, workstations, applications and any monitoring tools are enabled to monitor user activity.

> **Network Security**
>
> Our infrastructure servers reside behind high-availability firewalls and are monitored for the detection and prevention of various network security threats … . Next generation firewalls deployed within the data center as well as remote office sites monitor outbound communications for unusual or unauthorized activities … .

A. Change Management

128. As the term is used within the cybersecurity industry, "change management" refers to the process of managing changes to a company's IT systems—such as upgrading software or applying security patches to systems—to ensure the changes do not cause glitches, outages, or other unanticipated risks. This concept is distinct from "network monitoring," in the sense of monitoring a network for malicious threats.

129. Throughout the Relevant Period, SolarWinds had a formal change control process in place. As part of that process, the Company's routine practice was as follows: Network configuration changes would be submitted in the form of "Change Management Requests" or "CMRs," which would detail the scope of the proposed change and would be tracked through an internal ticketing System. Prior to implementation, the CMR would undergo two levels of approval: first by a manager, then by the "Change Administration Board" or "CAB"—a group composed of representatives from each major IT team at SolarWinds. Once a change was reviewed and approved by the CAB, the relevant IT team would roll out the change, monitoring for any problems and initiating a rollback if a significant problem was detected. Upon successful implementation of the approved change, the corresponding CMR ticket would be closed.

B. Auditing and Logging

130. SolarWinds is a manufacturer of network monitoring software, and among its offerings during the Relevant Period was a product called Security Event Manager or "SEM" (also referred to as Logging Event Manager or "LEM").

131. Security Event Manager ingests and monitors logs from systems on a network and generates alerts based on certain types of activity that can be customized in accordance with a particular user's needs.

132. SolarWinds used Security Event Manager to monitor systems on its own network.

133. Throughout the Relevant Period, SolarWinds generally configured network components, workstations, applications, and monitoring tools to transmit logs of user activity to Security Event Manager so the activity could be audited or monitored in real time for anomalous events.

134. On a daily basis, Security Event Manager logged tens or hundreds of millions of events at SolarWinds, including users logging on, applications being accessed, and files being read.

135. SolarWinds configured Security Event Manager to send email alerts to the InfoSec team based on the occurrence of certain types of security-related events, such as the adding of a user to a user group that had administrative privileges.

C. Network Security

136. "Firewalls" are network-security devices that monitor and control traffic flowing to and from a network, or to and from internal zones within a network. They can be configured to block or alert on traffic that fits certain criteria, such as traffic from a blacklisted IP address.

137. Throughout the Relevant Period, SolarWinds' routine practice was to use "next-generation firewalls" from Palo Alto Networks ("Palo Alto") to monitor both traffic to/from SolarWinds' network as well as traffic that traversed internal zones that SolarWinds maintained within its network.

138. These Palo Alto next-generation firewalls had advanced threat-detection capabilities that ordinary firewalls do not. As a part of the service it provided to SolarWinds, Palo

Alto would leverage its global network of firewalls—across all of its customers—to identify patterns of malicious conduct, and automatically update the attacker signatures and other heuristics that SolarWinds' firewalls would use to block or alert on potential malicious activity.

139. Palo Alto's next-generation firewalls generated "InfoSec Daily Monitoring Reports" for the SolarWinds InfoSec team, which listed various security events detected by the firewalls—such as the movement of large amounts of data, attempted traffic to a known malicious IP address, and other potentially harmful activity.

VII. SECURE DEVELOPMENT LIFECYCLE

140. Under the "Operational Security" heading, the Security Statement stated as follows:

> **Software Development Lifecycle**
>
> We follow a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of our products. Our products are deployed on an iterative, rapid release development lifecycle. Security and security testing are implemented throughout the entire software development methodology. Quality Assurance is involved at each phase of the lifecycle and security best practices are a mandated aspect of all development activities.
>
> Our secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments. The SolarWinds architecture teams review our development methodology regularly to incorporate evolving security awareness, industry practices and to measure its effectiveness.

141. The term "vulnerability testing" generally refers to the testing of software for vulnerabilities.

142. The term "regression testing" refers to checking that changes made to software code do not degrade software functionality that worked properly before the change. While this testing is not specific to security, it can identify software bugs with security implications.

143. The term "penetration testing" describes software testing that mimics real-world efforts by hackers to identify methods for circumventing the security features of an application.

144. SolarWinds routinely conducted vulnerability testing as part of its software development lifecycle during the Relevant Period.

145. Among other records of vulnerability testing, there are records of vulnerability scans of SolarWinds software being run through Checkmarx, a vulnerability scanning tool, during the Relevant Period as part of the software development process.

146. SolarWinds routinely conducted regression testing as a regular part of its software development lifecycle during the Relevant Period.

147. Among other records of such regression testing, there are records of tickets in JIRA (an internal workflow tracking tool used by SolarWinds software engineers) reflecting regression tests run on SolarWinds software during the Relevant Period as part of the software development process.

148. SolarWinds routinely conducted penetration testing as part of its software development lifecycle.

149. Among other records of such penetration testing, there are reports generated from BurpSuite (a penetration testing tool) reflecting penetration tests run on SolarWinds software during the Relevant Period as part of the software development process.

150. SolarWinds routinely conducted product security assessments as part of its software development lifecycle during the Relevant Period.

151. Vulnerability scans are a form of product security assessments.

152. Penetration tests are a form of product security assessments.

153. SolarWinds' development teams also often prepared product security assessments during the Relevant Period in the form of "Final Security Reviews" or "FSRs" that were prepared at the end of the software development process.

154. The Final Security Review was a document designed to collect in one place artifacts of security testing conducted during the development of a software release.

155. The FSRs would often contain, among other things, links to JIRA tickets containing assessments of potential code vulnerabilities that had been identified during development and information about how they had been mitigated or resolved.

156. During the Relevant Period, customers would sometimes send SolarWinds reports of potential vulnerabilities they had identified from scanning SolarWinds software or, more rarely, from conducting their own penetration tests. Customer support personnel would typically forward these reports to product development teams to evaluate whether the reports were false positives or not.

VIII. DOCUMENTS VIEWED BY THE SEC AS PERTAINING TO CERTAIN SECURITY STATEMENT REPRESENTATIONS[3]

A. Documents Viewed by the SEC as Pertaining to the Security Statement's Representation Relating to Following the NIST Cybersecurity Framework

157. On April 19, 2021, Kellie Pierce emailed Tim Brown and Andrea Anderson, attaching a document titled "SolarWinds Enterprise Policy and Procedures Documentation Audit Report Executive Summary DRAFT," dated April 12, 2021. [SW-SEC00185450-453]. The email stated in part, "Andrea performed an audit against the NIST 800-53 and generated a findings report for your review." [SW-SEC00185450]. The "Summary Conclusion" section in the attached document stated in part: "Overall, about 40% of the baseline controls within NIST were met or

[3] Under Federal Rule of Civil Procedure 901, the Parties agree that the documents in this section are authentic SolarWinds documents. The stipulations that follow, which were requested by the SEC, are strictly stipulations that the cited documents contain, in part, the quoted language. Defendants dispute the SEC's interpretation of these documents, and dispute their materiality, but intend to address these documents separately (including citing to other relevant language in the documents) in their own Statement of Undisputed Material Facts. The SEC reserves the right to rely upon other portions of these documents, or to rely upon other documents not cited in this stipulation, at summary judgment.

partially met within the policies reviewed. As of the date of testing, SolarWinds is still in the process of updating the policies and procedures and designing and implementing many of the NIST 800-53 recommended controls." [SW-SEC00185450 at 5451]. The document further stated: "The following chart represents further breakdown of the NIST controls and where improvements are needed." [SW-SEC00185452]. Below that the following chart appears:

	NIST 800-53 Control Family	Total Controls	% of controls Met
1	Access Control (AC)	43	63%
2	Awareness & Training (AT)	5	80%
3	Audit & Accountability (AU)	28	50%
4	Security Assessment and Authorization policies (CA)	12	50%
5	Configuration Management (CM)	31	6%
6	Contingency Planning (CP)	35	6%
7	Identification and Authentication (IA)	24	46%
8	Incident Response (IR)	16	56%
9	Maintenance (MA)	13	8%
10	Media Protection (MP)	12	42%
11	Physical and Environmental Protection (PE)	26	50%
12	Planning (PL)	6	100%
13	Personnel Security Policy and Procedures (PS)	9	56%
14	Risk Assessment (RA)	8	38%
15	System and Services Acquisition (SA)	19	26%
16	System and Communications Protection (SC)	35	26%
17	System and Information Integrity (SI)	21	67%
	Total	**343**	**40%**

B. Documents Viewed by the SEC as Pertaining to the Security Statement's Representations Relating to Role-Based Access Controls

158. Brad Cline, SolarWinds' Director of IT, prepared a June 2, 2017 presentation titled "Securing Active Directory." [SW-SEC00262012-2016 at 2013; B. Cline Dep. Tr. at 90:16–91:3; Ex. 5 to B. Cline Dep. Tr.]. The slide titled "Current assessment" in the June 2017 presentation

stated in part: "We have an unnecessary level of risk within our environment," and included three bullet points stating: "15 accounts running as Domain Admin"; "5 Domain Admin level service accounts with passwords unchanged as far back as 2007"; and "System team currently runs as Domain Admin, high level of risk during routine operations and particularly onboarding and off-boarding personnel." [SW-SEC00262012-2016 at 2013; Ex. 5 to B. Cline Dep. Tr.].

159. In an August 2017 PowerPoint titled "Monthly IT Leadership Meeting," a slide titled "A Proactive Security Model" included a bullet point under the heading "Risk of Non-Investment" stating: "[c]urrent state of security leaves us in a very vulnerable state for our critical assets. A compromise in these assets would damage our reputation and financially [sic]." [SW-SEC00259782 at 9788]. Another bullet point under that same heading stated: "Appropriate security policies, procedures, training, PEN testing are required by our commercial customers and asked for in qualifying questionnaires. Without appropriate answers we will lose business." [SW-SEC00259782 at 9788].

160. On a different slide of the August 2017 SolarWinds presentation, under the sub-heading "Risk Mitigation Plan for IT Security Operations," a bullet point stated: "[r]educe the number of security incidents by implementing industry standard best practices." [SW-SEC00259782 at 9787].

161. On September 7, 2017, Brown emailed a presentation stating in part the, "[c]urrent state of security and proposed move to a proactive security model." [SW-SEC00337355-7362 at 7355, 7356-7362]. A slide in this internal presentation included a bullet point under the heading "Risk of Non-Investment," which stated: "[c]urrent state of security leaves us in a very vulnerable state for our critical assets. A compromise in these assets would damage our reputation and financially [sic]." [SW-SEC00337355 at 7360].

162. This September 2017 presentation also contained cybersecurity areas that were color-coded in red: "Security training employee," "Data Classification," and "PEN Testing[.]" [SW-SEC00337355 at 7358]. This September 2017 presentation also stated in part that the "Lack of legally approved security questions/answers are costing us time and customers." [SW-SEC00337355 at 7359].

163. A December 14, 2017 email from Brown to CIO Rani Johnson attached a "Security 90 Day Review" prepared by Brown. [SW-SEC00262716-2743; T. Brown Dep. Tr. at 150:11-18]. The document contained a slide titled "State of Security Operations December 2017." For the category "Policies: Security, Data Retention, DR," the slide stated in part: "Policies are getting better with GDPR as a driver. Still more to do if we are going to measure ourselves against NIST or complete an ISO Audit. Still missing a number of standard policies." [SW-SEC00262716-2743 at 2721; T. Brown Dep. Tr. at 150:11–151:14].

164. The Security 90 Day Review attached to Brown's December 14, 2017 email to Rani Johnson also contained a slide titled "A proactive security model." [T. Brown Dep. Tr. at 156:22–157:1]. Under "Risks of non-investment," the slide included a bullet point stating: "Current state of security leaves us in a very vulnerable state for our critical assets. A compromise of those assets would damage our reputation and financially [sic]." [SW-SEC00262716-2743 at 2743; T. Brown Dep. Tr. at 156:22–158:10].

165. A January 2018 presentation prepared by a SolarWinds project manager and shared with Brown, as well as SolarWinds' CIO, Director of IT and others, stated in part that "Currently there is a collection of people who have access to many systems and many people involved in provisioning access." [SW-SEC00043618-3630 at 3618, 3621]. The presentation also stated in part: "The lack of standardized user access management processes that captures user provisioning

(hiring), user changes (transfer) and user de-provisioning (resignation and termination), across the organization create a loss risk of organizational assets and personal data." [SW-SEC00043618-3630 at 3621].

166. On June 4, 2018, Network Engineer Robert Krajcir emailed multiple people, including Brad Cline and Eric Quitugua, stating in part: "By this initiative, I would like to address the following problem: These days, we are in process of firewall cleanup and optimization, which showed us a security gap we are facing with our VPN service." [SW-SEC00031653-1668 at 1657]. Krajcir further stated: "What I propose: Use certificates for machine authentication. Basically it would mean, that users will only be able to connect to our VPN from verified/trusted devices, that are under IT control, joined the domain, are properly updated and have the required software properly installed and in use. For everyone else, there could be one or two separate VPN gateways per region with stricter policy (access to less resources)." [SW-SEC00031653 at 1657]. Krajcir attached a PowerPoint titled "BYOD solution, Machine certificate authentication," dated August 2018 (the "August 2018 BYOD Solution Presentation"), to his June 4, 2018 email. [SW-SEC00031653 at 1659-1668].

167. In a July 2018 blog post on security, Brown stated: "People often think of security as an insurance policy—something you have to have, like locks on your doors, fire and flood insurance, and business insurance. While these are all true, there are opportunities to think of security as a business enabler, something that can help you open additional doors for your business and stand out from your competition." [https://www.n-able.com/blog/10-steps-improved-cybersecurity-using-security-open-doors-your-business].

168. On August 24, 2018, Krajcir sent an email to Brad Cline and Eric Quitugua, stating: "To summarize the risk we are facing:

a. "Anyone with AD credentials can access our corporate wifi or corporate VPN from ANY device, no matter if [C]ompany owned or not." [SW-SEC00031653 at 1654].

b. "While on corporate wifi, or VPN, such device can basically do whatever without us detecting it until it's too late." [SW-SEC00031653 at 1654].

c. "It can easily download any content without being detected by [SolarWinds' data loss prevention software], which is normally installed on all domain PCs." [SW-SEC00031653 at 1654].

d. "[I]t can compromise entire network by spreading malware (spyware, viruses, trojans, ransomware), because we cannot ensure that such device will be fully compliant in terms of [operating system] updates, antivirus [protection], software installed etc." [SW-SEC00031653 at 1654].

169. On August 30, 2018, Krajcir forwarded the June 4, 2018 and August 24, 2018 emails from Krajcir and the August 2018 BYOD Solution Presentation to Eric Quitugua and others. [SW-SEC00594395].

170. On August 31, 2018, Eric Quitugua forwarded the June 4, 2018 and August 24, 2018 emails from Krajcir and the August 2018 BYOD Solution Presentation to Brown. [SW-SEC00594395-4400 at 4395].

171. A September 2018 "Incident Review" presentation contained various slides. [SW-SEC00386134-6143]. Under the slide "Security Program Status," "Identity Management – Role and Privilege Management," "Active Monitoring and true SOC services," and "Integration of Threat Intelligence" are color-coded in red which, according to the legend on the slide, means that they are "Limited or non existent". [SW-SEC00386134-6143 at 6143].

172. In October 2018, Brown prepared a draft presentation titled "Information Security - Risk Review." [SW-SEC00313351-3362; T. Brown Dep. Tr. at 163:8-23]. Under the slide "A Proactive Security Model – Updated October 2018 with status," it stated in part under the subheading "Risk of Non-Investment": "Current state of security leaves us in a very vulnerable state for our critical assets," color-coded in yellow; and "Lack of cyber hygiene leaves us open to being a target of opportunity and a compromise will create downtime and lost revenue," color-coded in green. [SW-SEC00313351-3362 at 3361]. This slide also stated under the subheading "Risk of Non-Investment," in part: "We have had 22 reported security incidents this year. Reactive responses cost significantly more than being proactive." [SW-SEC00313351-3362 at 3361].

173. On October 29, 2018, Brown sent an email to SolarWinds' CIO Rani Johnson which attached an "Information Security" PowerPoint dated October 2018. On a slide titled, "A Proactive Security Model – Updated October 2018 with status," the presentation stated in part: "Current state of security leaves us in a very vulnerable state for our critical assets. A compromise of these assets would damage our reputation and financially [sic]." It also stated: "We have had 22 reported security incidents this year. Reactive responses costs significantly more than being proactive." [SW-SEC00313350-3362 at 3361]. It further stated in part: "Without training our employees will continue to be one of our biggest risks." [SW-SEC00313350-3362 at 3361].

174. On June 28, 2019, Kellie Pierce sent an email to Brown, Rani Johnson, Chris Day, Brad Cline, and others in which she attached a spreadsheet titled "FedRAMP_Security_Controls_Baseline" [SW-SEC00151673; SW-SEC00045356; SW-SEC00218068]. The tab in the spreadsheet entitled "Moderate Baseline Controls" included Ms. Pierce's comments and notes regarding FedRAMP controls in the tab, which related to, among

other things, access controls, least privilege, and penetration testing. [SW-SEC00151673; SW-SEC00045356; SW-SEC00218068].

175. On August 28, 2019, Kellie Pierce sent an email to Brown, Rani Johnson, Chris Day, Brad Cline and others in which she attached a similar version of the "FedRAMP_Security_Controls_Baseline" spreadsheet. [SW-SEC00151673; SW-SEC00045356; SW-SEC00218068].

176. On September 25, 2019, Kellie Pierce sent an email to Brown, Rani Johnson, Chris Day, Brad Cline and others in which she attached a similar version of the "FedRAMP_Security_Controls_Baseline" spreadsheet. [SW-SEC00151673; SW-SEC00045356; SW-SEC00218068].

177. A SolarWinds August 16, 2019 Security & Compliance Program Quarterly Review, which Brown contributed to, contained what was titled: "SolarWinds Scorecard: NIST Maturity Level." [SW-SEC0001497-1550; T. Brown Dep. Tr. 183:13–184:20]. The scorecard for the "Protect" category included several bullet points under "Highlights," including: "Access and privilege to critical systems/data is inappropriate." [SW-SEC0001497 at 1507]. Also on the "Protect" scorecard, the "Security Category" "Authentication, Authorization and Identity Management," included the "Objective:" "User identity, authentication and authorization are in place and actively monitored across the company," with a "NIST Maturity Level" score of "1." [SW-SEC0001497 at 1507]. The maturity level of "1" was defined in the slide deck as: "The organization has an ad-hoc, inconsistent, or reactive approach to meeting the cybersecurity control objectives." [SW-SEC0001497 at 1507; T. Brown Dep. Tr. at 202:15–204:11; E. Quitugua Dep. Tr. at 284:18–287:4].

178. The SolarWinds August 16, 2019 Security & Compliance Program Quarterly Review contained a series of slides titled "Security & Compliances Initiatives." Another slide was titled "Financial: Enterprise Access Management (SOX Compliance)." On that slide, the Department of Operations & IT leads were Rick Homberg and Kellie Pierce and the executive sponsor was listed as Rani Johnson. Under the heading "Issues, Risks, and Dependencies," the slide contains notations stating: "[c]oncept of least privilege not followed as a best practice," "[u]se of shared accounts throughout internal and external applications," and "[p]roject scope expanded to include SOX compliance requirements." On the same slide under a subheading titled, "Action Required," the slide states: "ID existing permission levels within the enterprise," "[w]ork with teams to decommission use of shared accounts," and "[n]eed to assess existing control to ensure alignment with SOX requirements." [SW-SEC00001497 at 1523].

179. A November 15, 2019 SolarWinds Security & Compliance Program Quarterly Review, which Brown contributed to, contained a series of slides titled, "2019 Enterprise Security & Compliances Policy Review," and a slide titled "Security & Compliance Initiatives." [SW-SEC00001551-1581 at 1552; R. Brown Dep. Tr. at 222:3–223:2]. On a separate slide titled, "SolarWinds Security/Risk Scorecard," under the subheading "Key Asks/Plans in Progress," the slide listed several bullet points, including: "Effort to reduce Support's ability to easily access customer data;" "ITSM G-suite potentially externally exposes financial data;" and "Pushing forward with AD authentication guidelines for critical mission systems." [SW-SEC00001551-1581 at 1552]. That same slide listed a NIST maturity level of "2" under the "Identify" security category. [SW-SEC00001551-1581 at 1576; J. Bliss Dep. Tr. at 242:3–243:2]. The key on that slide defined a score of "2" as "Consistent approach, Somewhat reactive and undocumented." [SW-SEC00001551-1581 at 1576].

180. On January 16, 2020, Eric Quitugua, who had previously forwarded the August 2018 BYOD Solution Presentation from Krajcir to Brown in August 2018, sent Krajcir's emails to Brown again, and stated in part: "As you know, this did not get any traction, but wanted to share with you so that we can circle this back and see if we can re-assess and possibly implement some type of enforcement." [SW-SEC00666779-6784 at 6779; SW-SEC00594395-4400 at 4395; J. Bliss Dep. Tr. at 296:16–299:8].

181. A SolarWinds March 3, 2020 Quarterly Risk Review contained a SolarWinds "scorecard" for NIST Maturity Level. Under the heading "Key Risks," for "Protect" the scorecard listed "[s]ignificant deficiencies in user access management," and for "Identify" the scorecard stated, "[s]ecurity processes not consistently implemented." Under "Key Improvements" for "Protect" the scorecard listed "AD Authentication for critical systems." "AD" refers to "Active Directory." [SW-SEC00001608-1634 at 1611; T. Brown Dep. Tr. at 232:22–233:25, 237:5–239:12; J. Bliss Dep. Tr. at 246:18–254:2; R. Johnson Dep. Tr. at 226:16-23].

182. A SolarWinds May 22, 2020 Quarterly Risk Review contained a SolarWinds "scorecard" for NIST Maturity Level. Under the heading "Key Risks," for "Protect" the scorecard listed in part "[s]ignificant deficiencies in user access management." Under "1H 2020 Improvement Plan" for "Protect," the scorecard lists "Enforce AD Authentication for critical system." [SW-SEC00001602-1607 at 1605; E. Quitugua Dep. Tr. at 297:12–299:11; J. Bliss Dep. Tr. 254-4–257:15]. There was also a slide titled "Q1 2020 AD Access Audit Deficiency/Remediation" which contained a high-level summary of a Q1 2020 Active Directory access review audit. [SW-SEC00148267-8294 at 8283; J. Bliss Dep. Tr. at 256:16–257:15].

183. A SolarWinds October 27, 2020 Quarterly Risk Review contained a SolarWinds "scorecard" for NIST Maturity Level. Under the heading "Key Risks" for "Protect," the scorecard

listed "[s]ignificant deficiencies in user access management." Under the heading "Key Improvements" for "Protect," the scorecard listed "Continue to enable AD Authentication for critical systems." [SW-SEC00001582-1601 at 1587; T. Brown Dep. Tr. at 246:4–248:9; J. Bliss Dep. Tr. at 260:16–262:21].

C. Documents Viewed by the SEC as Pertaining to the Security Statement's Representations Relating to Passwords

184. A draft March 2018 Major Product Portfolio presentation contained a security projects slide presentation concerning "Enterprise Access Management (Standards & Audit)." [SW-SEC00042892-2964]. Eric Quitugua is listed as the DOIT lead for the project on slide No. 6 ("Enterprise Access Management (Standards & Audit)"), who contributed to this presentation. [SW-SEC-00042892 at 2907; E. Quitugua Dep. Tr. at 201:5–202:25.] Joseph Kim, Rani Johnson, and Brown are listed as executive sponsors. [SW-SEC-00042892 at 2907]. Slide No. 6 included notations under the heading "Issues, Risks, and Dependencies," stating: "Concept of least privilege not followed as a best practice" and "Use of shared accounts throughout internal and external applications." [SW-SEC00042892 at 2907]. Under the subheading "Action Required," the slide stated: "ID existing permission levels within the enterprise" and "Work with teams to decommission use of shared accounts." [SW-SEC00042892 at 2907; E. Quitugua Dep. Tr. at 218:20–220:20]. This is an earlier version of the same slide mentioned above in paragraph 178.

185. On April 13, 2018, Rani Johnson sent Brown, Eric Quitugua, and David Mills an email with the subject line: "Please follow up on Risk/Compensating Controls." It contains a table broken across several pages, in which three rows contain the entry: "Shared SQL legacy account login credentials used." On April 13, 2018, this email was forwarded to Brad Cline, Eric Quitugua, and Smitha Reddy. Brad Cline stated: "my understanding is these are old [SQL] accounts that are

shared among multiple [databases]/websites and pose a security risk". [SW-SEC00043080 at 080-083].

186. In November 2019, a SolarWinds employee sent an email to Chris Day and others about a request made by certain developers for certain access rights in connection with a project they were working on to improve SolarWinds' internal billing system, stating: "This request has brought to light three problems: They are currently using a shared login currently of a different SolarWinds employee. This is definitely a security incident and needs to stop. Solution – Granting the individual logins as requested." [SW-SEC00254254 at 265; *see also* same at 258 and 261]. Later in the email chain, this employee also stated in part: "When challenged it turns out they are all using a common login currently which is also not secure." [SW-SEC00254254 at 265; *see also* same at 258 and 261].

187. On November 19, 2019, SolarWinds' InfoSec team was notified by a security researcher that he had "found a public Github repo with is leaking ftp credential belongs to SolarWinds." The password was "solarwinds123." [SW-SEC00407702; SW-SEC00001464]. Both Mr. Brown and Mr. Quitugua described the password "solarwinds123" as "a very weak password," and Mr. Quitugua also testified that it lacked "complexity." [SW-SEC00407702 at 702; E. Quitugua Investigative Testimony, Vol. II at 360:16–361:25].

188. On March 2, 2020, Danielle Campbell emailed Chris Day, Rani Johnson, and others with the subject "SOX: Control Deficiencies FY19" and she attached an excel spreadsheet with the file name "FY2019 Deficiencies and Recommendations – Final." [SW-SEC00388330-8332 and attachment; J. Bliss Dep. Tr. at 257:22–260:7]. A slide titled "IT Issues noted during FY2019 Testing," contained a chart with the following totals next to the following categories: "[l]ack of evidence to show appropriate level of review"—11; "[p]assword requirements not being met

(Access)"—2; "[l]ack of access approval prior to provisioning (Access)"—3; "[a]ccess removal not being timely (Access)"—1. [Attachment to SW-SEC00388332]. The body of Ms. Pierce's email stated in part: "Hi, I wanted to send you an email to let you know that we have control deficiencies from our FY19 SOX Audit that will need to be remediated by your teams. I have set up meetings with the control owners over the next couple of weeks. The goal of these meetings will be to determine what remediation steps will be taken and how quickly they can be put in place." [SW-SEC00388330-8332 at 8330]. Ms. Pierce stated: "We have the Security & Compliance Quarterly Risk Review (QRR) meeting tomorrow with Jason Bliss and Bart Kalsu. We have a couple of slides dedicated to the SOX findings. I did not want it to be a surprise to you that these are included in that discussion." [SW-SEC00388330-8332 at 8330; J. Bliss Dep. Tr. at 258:19-25].

189. In a December 2020 email about the security researcher's discovery of the "solarwinds123" password, Mr. Brown stated in part: "I have assumed this was our main download site. … The point [the security researcher was] making was that they could have corrupted one of our downloads. … This was managed and resolved quickly but it did take place and a very weak password existed to access that environment." [SW-SEC00407702 at 702].

D. Documents Viewed by the SEC as Pertaining to the Security Statement's Representations Relating to Secure Development Lifecycle

190. On January 25, 2018, Steven Colquitt, SolarWinds Director of Software Development sent an email to SolarWinds engineering managers and others, that included the text of the portion of the SolarWinds's Security Statement entitled "Software Development Lifecycle," and wrote in part, "I think it's important that our engineering teams be aware of this which is a public facing security statement on Solarwinds.com. Please share with your teams." On January 30, 2018, he replied all to that email and stated:

> I've gotten feedback that we don't do some of the things that are indicated in the statement below. I want to make sure that you all have an answer to this.
>
> The simple response is: There is improvement needed to be able to meet the security expectations of a Secure Development Lifecycle. We will be working with teams throughout 2018 to begin incorporating the SDL into their development lifecycle. This begins with general SOL training for all of Engineering along with several SDL pilots with specific teams in Ql. We'll continue to pragmatically roll out the SDL to additional teams each quarter.
>
> Questions?
>
> [SW-SEC00238141-142].

191. In a May 21, 2018 email, Rani Johnson, SolarWinds Chief Information Officer, sent an email to Brown, copying Steven Colquitt, the Director of Software Development. The subject of the email was "Please confirm (particularly the threat modeling)." That same day, Colquitt responded: "I don't see a line item about threat modeling ... but since you mentioned it. TM'ing is a process. It's part of the SDL and we are just barely beginning to understand how teams are going to be doing this activity. So I am not sure what you are looking for in terms of confirmation." [SW-SEC00237608-609].

192. A 2018 PowerPoint presentation entitled "SolarWinds KBT Offsite DOIT and R&D," included a slide titled, "FY18 Initiatives." A row of a chart on the slide contains "PEN Testing" under the "Description" column and the following notation under "Notes": "Unfunded in FY18. Plan to PEN test 8-10 products in 2019." [SW-SEC00298924-8934 at 8934].

193. On February 13, 2019, August Wehrmann, a Vice President of Engineering over the MSP business unit, emailed "SW MSP Engineering All Staff," among others, including CTO Joe Kim. [SW-SEC-SDNY_00000004 (Ex. 7 to Kim Dep. Tr.) and Exs. 7A-7B]; J. Kim Dep. Tr. at 170:9–172:21]. Wehrmann attached a PowerPoint to his February 13 email titled "SolarWinds MSP R&D 2019 Kick-off," that was prepared by SolarWinds employees. [Ex. 7B to J. Kim Dep. Tr. at p. 1-27]. A slide in the presentation titled "Goal for FY19: Grow Together: Joe's Goals,

August's Goals, KPIs TBD[,]" stated in part: "Improve security both in our products and our positioning," "Audit MSP Engineering training level and adoption of SDL (Secure Development Lifecycle)," and "Drive down the number of incidents introduced by MSP Engineering." [Ex. 7B to J. Kim Dep. Tr. at p. 6; J. Kim Dep. Tr. at 176:16–183:3].

194. A SolarWinds May 17, 2019 Security & Compliance Program Quarterly Review stated on the slide entitled "Security: Security Incident Improvement Plan (SIIP)" under the "Description" heading: "Project to operationalize and improve overall security for SolarWinds. This effort includes training (security and SDL), department plans for addressing security, KPIs, and an annual audit to measure the effectiveness of security practices within SolarWinds." [SW-SEC00001635-1651 at 1650; T. Brown Dep. Tr. 177:2–179:10]. At the top of this slide, it stated: "Lead – Tim Brown" and "Executive Sponsor – Rani Johnson." [SW-SEC00001635-1651 at 1650].

195. A July 2019 document prepared by SolarWinds MSP employees Stas Starikevich and Wojciech Pitera, entitled "MSP Products Security Evaluation" stated in part under the heading "Summary Objectives": "Perform high level assessment of the operational maturity level that exists today for our key products – RMM, NCentral and Backup." [SW-SEC00166790-799 at 792; J. Bliss Dep. Tr. at 271:8-17]. Under the sub-heading "Methodology" it stated: "NIST, the Enterprise standard security Framework is being used to perform the assessments that will allow us to improve our ability to prevent, detect, and respond to cyber attacks." [SW-SEC00166790-799 at 792; J. Bliss Dep. Tr. at 271:18–272:15]. Under the heading "Communication and data flows are mapped" it stated: "Design documentation overall is lacking and unstructured for the majority products. In addition, there is no governance in place to help provide consistency. These are crucial for threat modelling [sic] & other security activities in SSDLC. This should be covered

by architecture, as part of the SSDLC process being formed." [SW-SEC00166790-799 at 793; J. Bliss Dep. Tr. at 272:16–275:22]. In the same document under the heading "Threats internal and external are identified and documented" it stated: "No threat modelling nor analysis is performed as part of any process (except MSP Backup Engineering). Has multiple pre-requirements to be implemented (external software assets, 3rd party systems list etc)." [SW-SEC00166790-799 at 794]. Under the sub-heading "Risk assessment (Identify)," this document stated: "Asset vulnerabilities are identified and documented. Each product seems to have its own ways of marking security issues that do not follow recently established SW standards." [SW-SEC00166790-799 at 794; J. Bliss Dep. Tr. at 275:23–276:18]. Under the sub-heading "Threat and vulnerability information is received from external sources," it stated: "Currently, there is no formal process in place for reporting purposes. It is recommended to have a process/framework to help provide guidance, specific to job responsibility/Role…(i.e. DevSecOps?") – A Pre-requirement to have a policy to maintain proper 3rd party asset list, OS versions utilized etc, to have data to work with." [SW-SEC00166790-799 at 794; J. Bliss Dep. Tr. at 276:19–277:19]. Under the subheading "Threats, vulnerabilities, likelihoods and impacts are used to determine risk," it stated: "No coverage due to missing pre requirements." [SW-SEC00166790-799 at 794; J. Bliss Dep. Tr. at 278:9–279:4].

196. A December 2019 document prepared by SolarWinds MSP employee Stas Starikevich entitled "MSP Products Security Evaluation MailAssure," stated under the heading "Threats internal and external are identified and documented": "No threat modelling nor analysis is performed as part of any process." [SW-SEC00283304 at 308].

197. A SolarWinds March 3, 2020 Quarterly Risk Review contained a SolarWinds "scorecard" for NIST Maturity Level. Under "Key Improvements," it listed "Increase SDL

adoption." [SW-SEC00001608-1634 at 1611; J. Bliss Dep. Tr. at 246:18–249:7]. In a different slide titled "Security & Compliance Improvement Plans (SCIPs)," in the third row titled "Dev-Ops/IT," it stated "[e]xpand pen testing program" under the column titled "Detect." [SW-SEC00001608-1634 at 1613; J. Bliss Dep. Tr. at 251:16–253:5].

198. A May 22, 2020 Q2 2020 Quarterly Risk Review stated under "1H 2020 Improvement Plan: "Increase SDL adoption." [SW-SEC00148267-8294 at 8270; J. Bliss Dep. Tr. at 254:4–257:15].

199. In a June 23–24, 2020 email chain between Brown, Johnson and others with the subject line, "SDL and Orion Improvement Program," a SolarWinds engineer stated in part "Do we have SDL process enforced for Orion Improvement Program server? If SDL is not enforced for OIP, we should do it ASAP and consider additional actions to make sure that OIP is very well protected." Another engineer responded, "I don't believe we cover OIP today with the SDL, but we should." [SW-SEC00000673-678].

200. A July 10, 2020 presentation titled, "PM Security Vulnerability & Incident Review" included several bullet points on a slide titled "ITOM Core Highlights and Asks" under the heading "Highlights," including: "Inconsistent internal security testing as part of product final security reviews don't always include web application testing before release"; and "Customers continue to actively engage 3rd party penetration testers as part of their compliance efforts[.]" [SW-SEC00006628-6648 at 6635; J. Bliss Dep. Tr. at 263:4–266:23].

/s/ Christopher J. Carney (with consent)[4]
Christopher J. Carney
Christopher M. Bruckmann
John J. Todor (*pro hac vice*)
Kirsten M. Warden (*pro hac vice*)
Benjamin Brutlag
Lorry Stone (*pro hac vice*)
U.S. SECURITIES AND EXCHANGE COMMISSION
100 F Street, N.E. Washington, D.C. 20549
Telephone: (202) 551-2379 (Carney)
Telephone: (202) 551-5986 (Bruckmann)
Telephone: (202) 551-5381 (Todor)
Telephone: (202) 551-4661 (Warden)
Telephone: (202) 551-5317 (Ney)
Telephone: (202) 551-2421 (Brutlag)
Telephone: (202) 551-4931 (Stone)
CarneyC@sec.gov
BruckmannC@sec.gov
TodorJ@sec.gov
WardenK@sec.gov
NeyW@sec.gov
BrutlagB@sec.gov
StoneL@sec.gov

Counsel for Plaintiff

/s/ Serrin Turner
Serrin Turner
Matthew Valenti
Nicolas Luongo
LATHAM & WATKINS LLP
1271 Avenue of the Americas
New York, NY 10020
Telephone: (212) 906-1200
Facsimile: (212) 751-4864
serrin.turner@lw.com
matthew.valenti@lw.com
nicolas.luongo@lw.com

Sean M. Berkowitz (*pro hac vice*)
LATHAM & WATKINS LLP
330 N. Wabash Avenue, Suite 2800
Chicago, IL 60611
Telephone: (312) 876-7700
Facsimile: (617) 993-9767
sean.berkowitz@lw.com

Counsel for Defendants SolarWinds Corp. and Timothy G. Brown

Alec Koch
KING & SPALDING LLP
1700 Pennsylvania Avenue, NW Suite 900
Washington, D.C. 20006
202-737-0500
akoch@kslaw.com

Counsel for Timothy G. Brown

[4] This electronic signature is used with consent in accordance with Rule 8.5(b) of the Court's ECF Rules and Instructions.